鳥取大学研究成果リポジトリ
Tottori University research result repository

タイトル Title	Authentication Based on Finger-Writing of a Simple Symbol on a Smartphone
著者 Auther(s)	Takahashi, Atsushi; Nakanishi, Isao
掲載誌・巻号・ページ Citation	Proceedings of 2018 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS2018) : 411 - 414
刊行日 Issue Date	2018-11
資源タイプ Resource Type	会議資料 / Conference Paper
版区分 Resource Version	著者版 / Author
権利 Rights	© © 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
DOI	
URL	http://repository.lib.tottori-u.ac.jp/6287

Authentication Based on Finger-Writing of a Simple Symbol on a Smartphone

Atsushi Takahashi
Graduate School of Engineering
Tottori University
Tottori, Japan
Email: b14t3035@eecs.tottori-u.ac.jp

Isao Nakanishi
Factory of Engineering
Tottori University
Tottori, Japan
Email: nakanishi@tottori-u.ac.jp

***Abstract*— For personal authentication of smartphone users, a convenient method, e.g., the use of a password that employs several digits or fingerprint authentication, is generally used. However, through these methods, we cannot precisely identify whether the person who poses as the user is actually the genuine one. Therefore, we propose a personal-authentication method based on finger-writing of a simple symbol, which considers both usability and security, and evaluate the verification performance of this system. As a result, the best equal error rate of 10% was achieved.**

Keywords— authentication, finger- writing, smartphone, simple symbol

I. INTRODUCTION

Authentication systems that use passwords and fingerprints are introduced for personal authentication of smartphone. The former is a simple authentication method because only several digits are input. However, the passwords of users suffer from a high risk of identity theft due to password leakage.

Fingerprint authentication is called biometrics. Biometric authentication is classified into two types, according to the authentication features. One is the use of physical features, such as fingerprints and faces and the other is the use of behavioral features, such as signatures and voices. In the biometrics process that uses physical features, biometric data are always exposed on the body surface; therefore, users can easily present them to the authentication system. Fast authentication and high usability can be achieved with high authentication accuracy. On the other hand, there is the risk that biometric data can be easily stolen by others because they are always exposed on the body surface. Even if they are leaked, they cannot be changed, in contrast to the use of a password. A security problem, therefore, exists. In the methods that use behavioral features, the biometric information is not exposed to the outside and the confidentiality of features is higher than the methods that use physical features. Therefore, we can consider that the authenticity of the process is better than using physical features. However, their authentication accuracy is low because behavioral features vary at every measurement.

The authors of the current study focused on writer authentication, which is a behavioral based biometric. However, conventional writer authentication suffers from the fact that authentication time is relatively long because users must write their names or specific characters using a pen. To create handwriting authentication with the highest usability, we proposed a method of finger- writing a simple symbol on a smartphone.

II. AUTHENTICATION BY FINGER WRITING A SIMPLE SYMBOL

Conventional writing authentication is achieved by signature verification [1], [2], text-indicated verification [3], [4], free writing verification [5] and these are classified according to two viewpoints: “text-dependent or independent” and “system-dependent or independent”. Table 1 lists these classifications.

Table 1. Classifications of writer authentication methods

		System: Independent	System: Dependent
Text	Dependent	Signature Verification	Text Indicated Verification
Text	Independent	Free Writing Verification	?

“Signature verification” is “system-independent” and “text-dependent”. Due to the fact that the writing content comes from a user name, it is not determined by the system and is dependent on the user. Other writer authentication methods can also be similarly classified. Table 2 lists a comparison of the usability and security in writer authentication methods. If these methods are applied in the use of smartphones, they are unsuitable because of low usability.

Table 2. Comparison of writer authentication methods

Authentication method	Usability	Security
Signature Verification	△	×
Free Writer Verification	×	○
Text Indicated Verification	×	△

However, there is not methods belongs to the "system-dependent" and "text-independent" classification ("?" in Table 1). In the method that is "system-dependent" and "text-independent," we assume that the authentication system specifies that the written contents are not related to the user. Further, the authentication system designates different writing contents every time authentication is required. In addition, identifying the person that writes the content is difficult. Thus, the security of this method is high.

III. Proposed Method

We focus on determining "?" from Table 1 and propose a new method based on finger-writing a simple symbol. The proposed method allows for authentication by writing a simple symbol such as ○, △, or □ using a finger on the screen of a smartphone. In the "?" method, the written content must be unrelated to the user. In other words, by adopting a worldwide known symbol, "system dependence" and "text independence" are simultaneously established. As a result, by writing a simple symbol, the writing time can be considerably shortened compared with that in the conventional method. Thus, the poor usability was improved.

Two types of features can be extracted from handwriting: "offline" and "online" features. The offline features are coordinate information obtained from the finger position on the screen during handwriting. The online features are the writing pressure and writing time taken for the finger-writing motion.

1) Offline features

- Average values of the coordinates of X and Y
- Maximum values of the coordinates of X and Y
- Minimum values of the coordinates of X and Y
- Difference in the values of the coordinates of X and Y
- Distance between the starting and ending points
- Drawing area
- Coordinates of the starting and ending points

2) Online features

- Average values of the finger pressure and contact area
- Maximum values of the finger pressure and contact area and their coordinates
- Minimum values of the finger pressure and contact area and their coordinates
- Average values of the velocity and acceleration
- Maximum values of the velocity and acceleration and their coordinates
- Minimum values of the velocity and acceleration and their coordinates
- Velocities near the starting and ending points (Derived from the five sampling data before and after relative to the start- and end-point coordinates)
- Acceleration near the starting and ending points
- Finger pressure on the starting and ending points
- Contact areas of the starting and ending points
- Writing time

IV. Experiment and Results

We derived the authentication performance of each symbol using the aforementioned features and investigated the individuality of each feature.

A. Finger-writing environment

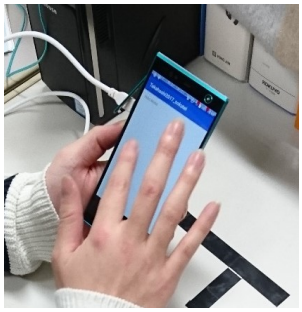
In this experiment, the authors used "ARROWS NX" of an Android smartphone. During finger–writing, the effect of the specific operating manner of the smartphone on the authentication performance is considered. Therefore, we investigated the difference in the authentication performance of the operating manner using the following three methods:

1) A method that places a smartphone on a desk in front of the user and performing finger-writing using the finger of a dominant hand

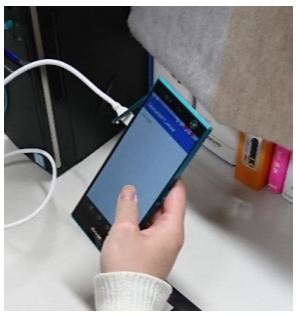
2) A method that places a smartphone in front of the user and performing finger-writing using the finger of a dominant hand

3) A free-finger-writing method by each subject

(a) *Method (1)*



(b) *Method (2)*



(c) *Method (3)*

Fig.1 Three methods assuming different finger-writing environments.

Figure 1 shows three methods of the finger-writing environments. Nineteen subjects randomly wrote ○, △, and □ on a smartphone screen 20 times. The influence on the authentication performance due to the different finger-writing environments and techniques was investigated.

B. Verification

Euclidean distance was used for the verification method. Among the 20 data sets, 10 sets of data from the first trials were averaged and then used as a template for the verification. The other 10 data sets were used as verification data. Equal error rate (EER) was used to evaluate the verification performance.

Table 3. EERs of each symbol in the feature (offline: left, online: right)

Features	Symbol	EER(%)			Features	Symbol	EER(%)		
		Method (1)	*Method (2)*	*Method (3)*			*Method (1)*	*Method (2)*	*Method (3)*
Average value of coordinate of X	○	40.8	40.0	**37.4**	Average value of finger pressure	○	35.6	32.6	28.9
	△	44.2	45.2	41.5		△	34.7	32.6	29.3
	□	41.1	44.1	42.1		□	33.2	33.1	**27.2**
Average value of coordinate of Y	○	32.4	30.5	**30.0**	Average value of contact area	○	32.5	28.9	25.8
	△	35.3	35.5	34.2		△	32.6	28.4	25.2
	□	36.3	35.5	31.9		□	31.9	31.6	**23.1**
Maximum value of coordinate of Y	○	**29.9**	31.1	32.6	Maximum value of finger pressure	○	33.4	30.4	27.2
	△	32.9	32.0	33.5		△	33.4	30.1	23.1
	□	34.2	33.7	30.4		□	31.6	31.5	**22.4**
Minimum value of coordinate of X	○	34.1	32.6	**28.9**	Coordinate of the finger pressure maximum value	○	32.1	**31.0**	31.5
	△	35.1	29.3	32.6		△	33.2	34.2	40.0
	□	36.8	34.7	36.1		□	37.2	34.7	34.0
Minimum value of coordinate of Y	○	30.8	28.4	26.7	Average value of velocity	○	30.5	27.2	**25.7**
	△	33.7	28.2	29.5		△	27.9	27.2	27.9
	□	30.5	29.5	**25.6**		□	27.4	27.3	28.2
Drawing area	○	27.4	27.4	25.7	Average value of acceleration	○	35.2	31.4	28.4
	△	27.4	27.8	27.3		△	30.0	**26.8**	33.7
	□	26.8	**24.2**	27.9		□	27.2	29.5	32.1
Coordinate of the starting point	○	26.3	25.1	27.7	Maximum value of velocity	○	35.3	32.6	29.5
	△	30.0	27.3	25.8		△	30.5	**27.9**	34.2
	□	26.2	23.1	**19.5**		□	32.0	34.7	37.9
Coordinate of the ending point	○	27.2	29.3	28.9	Writing time	○	26.8	27.9	**25.2**
	△	31.5	28.4	28.4		△	27.9	27.1	28.1
	□	26.8	24.7	**18.4**		□	29.2	27.7	27.9

C. Results

Table 3 lists a part of the EERs of each feature in each symbol. The smallest EERs are presented in bold face. From the results, we believe that data below 30% exhibited individuality. In particular, the coordinate features of the starting and ending points achieved better results, which were less than 20%, and we could assume that individuality exists in the stroke order of the symbols (whether one wrote ○ from the top and others wrote it from the bottom). Furthermore, we can say that individuality exists in the size of the symbols because relatively good results were obtained in the drawing area. In addition, by comparing the three environments, relatively good results were obtained in *Method (3)*. We can state, therefore, that the free-writing method such as *Method (3)* is suitable for extraction of individuality, because we can assume that individuality is lost in the writing methods according to a certain rule, such as that in *Methods (1) and (2)*.

To improve the authentication performance, the above features were combined. To eliminate the difference in the feature quantities, normalization was introduced using the following equation:

$$Y = (X - Xmin) / (Xmax - Xmin) \qquad (1),$$

where:

- Y : normalized data
- X : original data
- $Xmin$: minimum value of the original data
- $Xmax$: maximum value of the original data

The normalized data derived from Eq. (1) were merged at the feature level. The following are the combined features:

- Combination of the offline, online and all features
- Combination of the finger-pressure features
- Combination of the contact-area features
- Combination of the velocity features
- Combination of the acceleration features
- Combination of the starting-point features
- Combination of the ending-point features
- Combination of the features that give good results in ○, △, or □
- Combination of the TOP-3 features that give good results for ○ or □

The use of coordinate features, such as the coordinate of the maximum value of the finger pressure in our experiment, did not yield an improved authentication performance. Therefore, we believe that the combination of the finger pressure, contact area, velocity, and acceleration features with a coordinate feature caused the authentication performance to improve. Thus, we conducted a survey to determine better combinations. For example, we derived the EERs in cases where the coordinate feature was included and excluded about the finger pressure, contact area, velocity, and acceleration features.

Table 4. EERs by combining features in each symbol.

Combination	Symbol	EER(%)	Combination	Symbol	EER(%)	Combination	Symbol	EER(%)
Offline features	○	**13.2**	TOP 3 of O	○	**15.3**	Velocity feature (1)	○	**25.2**
	△	15.7		△	17.6		△	28.4
	□	15.2		□	17.2		□	29.3
Online features	○	**16.8**	TOP 3 of □	○	18.8	Velocity feature (2)	○	**26.8**
	△	21.0		△	14.2		△	35.3
	□	17.2		□	**10.0**		□	35.2
All features	○	12.5	Finger pressure feature (1)	○	**22.6**	Acceleration feature (1)	○	34.2
	△	13.2		△	26.3		△	36.6
	□	**11.6**		□	25.2		□	**34.0**
Good results of O	○	**11.6**	Finger pressure feature (2)	○	19.5	Acceleration feature (2)	○	**34.0**
	△	21.4		△	25.1		△	45.2
	□	18.2		□	**18.4**		□	38.4
Good results of △	○	33.5	Contact area feature (1)	○	23.1	Starting point feature	○	24.6
	△	**26.3**		△	22.1		△	26.8
	□	29.3		□	**19.8**		□	**22.0**
Good results of □	○	14.6	Contact area feature (2)	○	**20.5**	Ending point feature	○	19.4
	△	14.7		△	24.7		△	16.7
	□	**11.0**		□	21.6		□	**11.6**

Table 4 lists the EERs derived by combining the features. Because *Method (3)* demonstrated the best individuality in Table 3, the results in Table 4 were obtained from *Method (3)*. The smallest EER at each feature is shown in bold face.

The desired best result was to obtain an EER of 10.0% when the features of TOP 3 of □ were combined, which was the combined coordinate of the starting point, coordinate of the end point, and maximum value of the finger pressure. All of these features exhibited high authentication performance, even during this experiment. Therefore, we found that the authentication performance is improved if the feature shows strong individuality, even with the use of few combinations.

The finger pressure feature has the following characteristics: (1) it does not include the coordinate feature, and (2) includes the coordinate feature. The other features are similar. Feature (1) provided better results, but Feature (2) contained the coordinate feature: therefore, it yielded no good results. Overall, the coordinate feature had poor authentication performance , as listed in Table 3. Because these coordinate features were obtained without being normalized with the coordinate position of the symbol, the individual differences in the coordinate feature were bad data, and resulted in poor authentication performance.

The combination of offline, online and all features provided good results. In addition, better results were obtained, even at TOP3 of ○ and □, and good results were obtained from the combination of ○ and □. But with regard to △, a worse result was achieved compared with the others. Due to the fact that all subjects had difficulty writing △ on a smartphone, we believed that variations in the feature were present, even among genuine users. Therefore, a good EER was not obtained for any features. In addition, because only three features that provided the best results for △, were considered, we did not consider TOP 3 of △.

V. Conclusion

We have proposed finger-writing a simple symbol as a new authentication method for smartphones. In this method, we used features with higher security than fingerprints during the writing. In addition, to make the system more convenient than the conventional system, a simple symbol was written. We derived the EERs by Euclidean distance matching using various features obtained from the finger-writing on the screen of a smartphone. Moreover, we aimed to derive better EERs by combining the features. From the best results, an EER of 10.0% was obtained the combined feature of Top 3 of □. For future investigation, we will revise the individual features and combine them. Furthermore, processing the finger-writing data as time-series data and verifying them using the DP (dynamic programing) matching will be carried out to improve the model suggested herein.

References

[1] T. Yoshida, S. Hangai, "Mobile Writer Verification using a Sequence of Touching Durations in Writing Characters," Proc. of IPCT, pp. 17-21, April 2015.

[2] T. Yoshida, Y. Tanaka, S. Hangai, "A Study on Signature/ Sign Authentication with Touching Information on Smart Phone," ICBBT'17 Proceedings of the 9th International Conference on Bioinformatics and Biomedical Technology, pp. 80-83, 2017

[3] Y. Yamazaki, N. Komatsu, "A Study on Text-Indicated Writer Verification," IEICE. PRMU-97(112), pp. 39-46, June 1996.

[4] K. Tsubota, K. Masuda, S. Hangai, "A Study on Authentication System using the Coordinates and Writing Speeds of Segments Extracted from Sign Strokes on Tablet," IEICE, BioX2016-13, vol. 182, pp. 33-38, August 2016.

[5] K. Matsuda, W. Ohyama, T. Wakabayashi, "Generalized Combined Segmentation-Verification for Multi-Script Signatures using Random-Impostor Training," IEICE, BioX2016-14, vol. 182, pp. 39-43, August 2016.